How not to be scammed online this Black Friday

By Maeson Maherry

25 Nov 2020

The appetite for online shopping reaches its peak this Black Friday for discount-hungry customers, and while buyers and businesses seek to capitalise on the shopping craze, cybercriminals, too, will be on the lookout for unsuspecting shoppers.

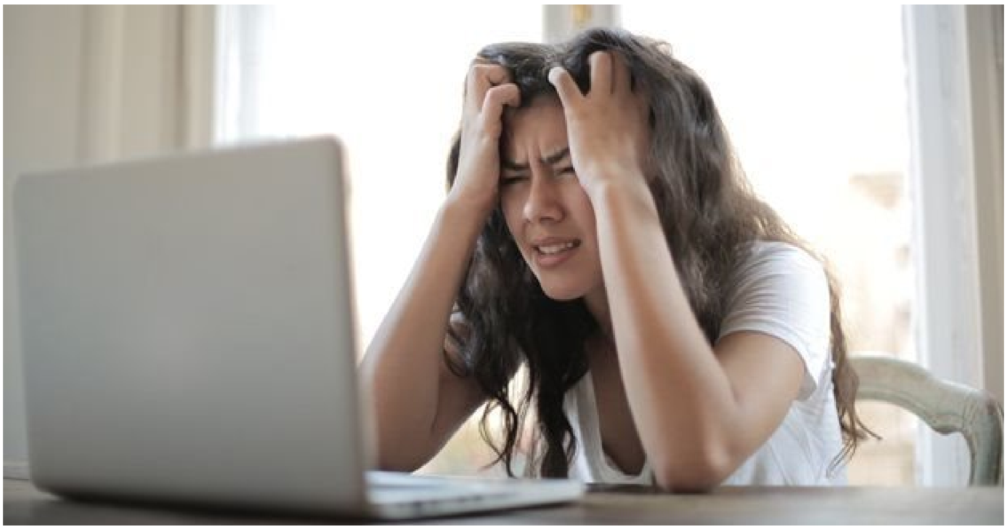

Photo by Andrea Piacquadio from Pexels

The coronavirus pandemic has changed the way we prefer shopping: Having worked and shopped remotely during most of this year has made us comfortable with using cyber tools.

The biggest threats we are facing are impersonation and phishing. Impersonation is when cyber attackers send emails that attempt to impersonate an individual or company for gaining access to sensitive and confidential information; while phishing is when one attempts to obtain sensitive information or data, such as usernames, passwords, and credit card details, by disguising themselves as a trustworthy entity in any electronic communication.

With Black Friday approaching, fraudsters are again stepping up their efforts to take advantage of consumers searching for bargains. It's easy to impersonate people and websites when you are online. We need to be able to identify fake sites.

To stay safe during Black Friday, you need first to learn what strategies scammers commonly use to take advantage of customers shopping online. By taking the right precautions, such as avoiding clicking suspicious links and not doing your online shopping on public Wi-Fi, you are much less likely to become the victim of an online scam.

Odd URLs, 'merchants', and HTTPS encryption

Remember: it is always better to go directly to the retailer's website to verify any deals that you see across social media platforms.

Instead of rushing to click on whatever 'deal' on offer, be sure to type the retailer's URL into your browser's address bar to verify that the bargain is authentic. Ensure that all your shopping takes place on legitimate tried-and-tested websites: be wary of odd URLs and stay away from "merchants" offering suspiciously cheap items.

Before you input your personal and payment details on a business site, ensure that it uses HTTPS web encryption, so that all the information that passes between your browser and the website is encrypted and prying eyes can't see and interfere with it. If the website is encrypted, a padlock icon on the left side of your browser's URL bar will indicate. When clicked on, it will verify that your connection to the site is secure.

6 ways to safeguard yourself this Black Friday, Cyber Monday

Nithen Naidoo 17 Nov 2020

Keep your operating system and applications updated with the latest security patches to reduce the number of openings through which attackers can compromise your machine.

When making online transactions, consider the risks when a retailer asks for permission to store your card details on their site. While it is convenient to store your credit card information, you need to weigh the retailers' ability to keep your information safe against the ingenuity of hackers.

It is important to be cyber streetwise and understand how exactly you could be tricked into an online credit card fraud and learn the ways to lower your risk. By reading around the impact credit card fraud can have, you are more likely to think twice before rushing into an impulse purchase that plays into the hands of a scammer.

ABOUT THE AUTHOR

Maeson is CEO of Law Trust.